Foundation of Cryptography, Lecture 8
Encryption Schemes

Iftach Haitner, Tel Aviv University

Tel Aviv University.

June 04, 2013

Section 1

Definitions

Correctness

Definition 1 (encryption scheme)

A trippet of PPTM's $(\mathsf{G}, \mathsf{E}, \mathsf{D})$ such that

1. $\mathsf{G}(1^n)$ outputs $(e, d) \in \{0,1\}^* \times \{0,1\}^*$
2. $\mathsf{E}(e, m)$ outputs $c \in \{0,1\}^*$
3. $\mathsf{D}(d, c)$ outputs $m \in \{0,1\}^*$

Correctness: $\mathsf{D}(d, \mathsf{E}(e, m)) = m$, for any $(e, d) \in \mathrm{Supp}(\mathsf{G}(1^n))$ and $m \in \{0,1\}^*$

Correctness

Definition 1 (encryption scheme)

A trippet of PPTM's $(\mathsf{G}, \mathsf{E}, \mathsf{D})$ such that

1. $\mathsf{G}(1^n)$ outputs $(e, d) \in \{0,1\}^* \times \{0,1\}^*$
2. $\mathsf{E}(e, m)$ outputs $c \in \{0,1\}^*$
3. $\mathsf{D}(d, c)$ outputs $m \in \{0,1\}^*$

Correctness: $\mathsf{D}(d, \mathsf{E}(e, m)) = m$, for any $(e, d) \in \mathsf{Supp}(\mathsf{G}(1^n))$ and $m \in \{0,1\}^*$

Correctness

Definition 1 (encryption scheme)

A trippet of PPTM's $(\mathsf{G}, \mathsf{E}, \mathsf{D})$ such that

1. $\mathsf{G}(1^n)$ outputs $(e, d) \in \{0,1\}^* \times \{0,1\}^*$
2. $\mathsf{E}(e, m)$ outputs $c \in \{0,1\}^*$
3. $\mathsf{D}(d, c)$ outputs $m \in \{0,1\}^*$

Correctness: $\mathsf{D}(d, \mathsf{E}(e, m)) = m$, for any $(e, d) \in \mathrm{Supp}(\mathsf{G}(1^n))$ and $m \in \{0,1\}^*$

- e – encryption key, d – decryption key
- m – plaintext, $c = \mathsf{E}(e, m)$ – ciphertext
- $E_e(m) \equiv E(e, m)$ and $D_d(c) \equiv D(d, c)$,

Correctness

Definition 1 (encryption scheme)

A trippet of PPTM's $(\mathsf{G}, \mathsf{E}, \mathsf{D})$ such that

1. $\mathsf{G}(1^n)$ outputs $(e, d) \in \{0,1\}^* \times \{0,1\}^*$
2. $\mathsf{E}(e, m)$ outputs $c \in \{0,1\}^*$
3. $\mathsf{D}(d, c)$ outputs $m \in \{0,1\}^*$

Correctness: $\mathsf{D}(d, \mathsf{E}(e, m)) = m$, for any $(e, d) \in \mathrm{Supp}(\mathsf{G}(1^n))$ and $m \in \{0,1\}^*$

- e – encryption key, d – decryption key
- m – plaintext, $c = \mathsf{E}(e, m)$ – ciphertext
- $E_e(m) \equiv E(e, m)$ and $D_d(c) \equiv D(d, c)$,
- public/private key

Security

- What would we like to achieve?

Security

- What would we like to achieve?

Security

- What would we like to achieve?
- Attempt: for any $m \in \{0,1\}^*$:

$$(m, E_{(G(1^n))_1}(m)) \equiv (m, U_{\ell(|m|)})$$

Security

- What would we like to achieve?
- Attempt: for any $m \in \{0,1\}^*$:

$$(m, E_{(G(1^n)_1)}(m)) \equiv (m, U_{\ell(|m|)})$$

Security

- What would we like to achieve?
- Attempt: for any $m \in \{0,1\}^*$:

$$(m, E_{(G(1^n))_1}(m)) \equiv (m, U_{\ell(|m|)})$$

  - Shannon – only for m with $|m| \leq |G(1^n)_1|$

Security

- What would we like to achieve?
- Attempt: for any $m \in \{0,1\}^*$:

$$(m, E_{(G(1^n))_1}(m)) \equiv (m, U_{\ell(|m|)})$$

  - Shannon – only for m with $|m| \leq |G(1^n)_1|$

Security

- What would we like to achieve?
- Attempt: for any $m \in \{0,1\}^*$:

$$(m, E_{(G(1^n))_1}(m)) \equiv (m, U_{\ell(|m|)})$$

  - Shannon – only for m with $|m| \leq |G(1^n)_1|$
  - Other concerns, e.g., multiple encryptions, active adversary

Semantic Security

1. Ciphertext reveals “no information" about the plaintext

Semantic Security

1. Ciphertext reveals “no information" about the plaintext
2. Formulate via the simulation paradigm

Semantic Security

1. Ciphertext reveals “no information" about the plaintext
2. Formulate via the simulation paradigm
3. Cannot hide the message length

Semantic security – private-key model

Definition 2 (Semantic Security – private-key model)

An encryption scheme $(\mathsf{G}, \mathsf{E}, \mathsf{D})$ is semantically secure in the private-key model, if $\forall$ PPTM A, $\exists$ PPTM A' s.t. the following holds: $\forall$ poly-length dist. ensemble $\mathcal{M} = \{\mathcal{M}_n\}_{n\in\mathbb{N}}$ and poly-length functions $h, f \colon \{0,1\}^* \mapsto \{0,1\}^*$

$$\Big| \Pr_{m\leftarrow\mathcal{M}_n, e\leftarrow G(1^n)_1}[\mathsf{A}(1^n, 1^{|m|}, h(1^n, m), E_e(m)) = f(1^n, m)] - \Pr_{m\leftarrow\mathcal{M}_n}[\mathsf{A}'(1^n, 1^{|m|}, h(1^n, m)) = f(1^n, m)] \Big| = \operatorname{neg}(n)$$

Semantic security – private-key model

Definition 2 (Semantic Security – private-key model)

An encryption scheme (G, E, D) is semantically secure in the private-key model, if $\forall$ PPTM A, $\exists$ PPTM A' s.t. the following holds: $\forall$ poly-length dist. ensemble $\mathcal{M} = \{\mathcal{M}_n\}_{n\in\mathbb{N}}$ and poly-length functions $h, f\colon \{0,1\}^* \mapsto \{0,1\}^*$

$$\Bigl| \Pr_{m\leftarrow\mathcal{M}_n, e\leftarrow G(1^n)_1}[A(1^n, 1^{|m|}, h(1^n, m), E_e(m)) = f(1^n, m)] - \Pr_{m\leftarrow\mathcal{M}_n}[A'(1^n, 1^{|m|}, h(1^n, m)) = f(1^n, m)] \Bigr| = \operatorname{neg}(n)$$

- Non-uniform definition

Semantic security – private-key model

Definition 2 (Semantic Security – private-key model)

An encryption scheme $(\mathsf{G}, \mathsf{E}, \mathsf{D})$ is semantically secure in the private-key model, if $\forall$ PPTM A, $\exists$ PPTM A' s.t. the following holds: $\forall$ poly-length dist. ensemble $\mathcal{M} = \{\mathcal{M}_n\}_{n \in \mathbb{N}}$ and poly-length functions $h, f \colon \{0,1\}^* \mapsto \{0,1\}^*$

$$\Big| \Pr_{m \leftarrow \mathcal{M}_n, e \leftarrow G(1^n)_1} [\mathsf{A}(1^n, 1^{|m|}, h(1^n, m), E_e(m)) = f(1^n, m)] - \Pr_{m \leftarrow \mathcal{M}_n} [\mathsf{A}'(1^n, 1^{|m|}, h(1^n, m)) = f(1^n, m)] \Big| = \operatorname{neg}(n)$$

- Non-uniform definition
- public-key variant — A and A' get e

Semantic security – private-key model

Definition 2 (Semantic Security – private-key model)

An encryption scheme $(\mathsf{G}, \mathsf{E}, \mathsf{D})$ is semantically secure in the private-key model, if $\forall$ PPTM A, $\exists$ PPTM A' s.t. the following holds: $\forall$ poly-length dist. ensemble $\mathcal{M} = \{\mathcal{M}_n\}_{n\in\mathbb{N}}$ and poly-length functions $h, f \colon \{0,1\}^* \mapsto \{0,1\}^*$

$$\left| \Pr_{m\leftarrow\mathcal{M}_n, e\leftarrow G(1^n)_1}[\mathsf{A}(1^n, 1^{|m|}, h(1^n, m), E_e(m)) = f(1^n, m)] - \Pr_{m\leftarrow\mathcal{M}_n}[\mathsf{A}'(1^n, 1^{|m|}, h(1^n, m)) = f(1^n, m)] \right| = \operatorname{neg}(n)$$

- Non-uniform definition
- public-key variant — A and A' get e
- Reflection to $\mathcal{ZK}$

Semantic security – private-key model

Definition 2 (Semantic Security – private-key model)

An encryption scheme $(\mathsf{G}, \mathsf{E}, \mathsf{D})$ is semantically secure in the private-key model, if $\forall$ PPTM A, $\exists$ PPTM A' s.t. the following holds: $\forall$ poly-length dist. ensemble $\mathcal{M} = \{\mathcal{M}_n\}_{n\in\mathbb{N}}$ and poly-length functions $h, f \colon \{0,1\}^* \mapsto \{0,1\}^*$

$$\Big| \Pr_{m\leftarrow\mathcal{M}_n, e\leftarrow G(1^n)_1}[\mathsf{A}(1^n, 1^{|m|}, h(1^n, m), E_e(m)) = f(1^n, m)] - \Pr_{m\leftarrow\mathcal{M}_n}[\mathsf{A}'(1^n, 1^{|m|}, h(1^n, m)) = f(1^n, m)] \Big| = \operatorname{neg}(n)$$

- Non-uniform definition
- public-key variant — A and A' get e
- Reflection to $\mathcal{ZK}$
- We sometimes omit 1^n , $1^{|m|}$

Indistinguishablity of encryptions

- The encryption of two strings is indistinguishable

Indistinguishablity of encryptions

- The encryption of two strings is indistinguishable

Indistinguishablity of encryptions

- The encryption of two strings is indistinguishable
- Less intuitive than semantic security, but easier to work with

Definition 3 (Indistinguishablity of encryptions – private-key model)

An encryption scheme $(\mathsf{G}, \mathsf{E}, \mathsf{D})$ has indistinguishable encryptions in the private-key model, if for any $p, \ell \in \text{poly}$, $\{x_n, y_n \in \{0,1\}^{\ell(n)}\}_{n \in \mathbb{N}}$ and $\{z_n \in \{0,1\}^{p(n)}\}_{n \in \mathbb{N}}$

$$\{(z_n, E_e(x_n))_{e \leftarrow G(1^n)_1}\}_{n \in \mathbb{N}} \approx_c \{(z_n, E_e(y_n))_{e \leftarrow G(1^n)_1}\}_{n \in \mathbb{N}}$$

Indistinguishablity of encryptions – private-key model

Definition 3 (Indistinguishablity of encryptions – private-key model)

An encryption scheme $(\mathsf{G}, \mathsf{E}, \mathsf{D})$ has indistinguishable encryptions in the private-key model, if for any $p, \ell \in \text{poly}$, $\{x_n, y_n \in \{0,1\}^{\ell(n)}\}_{n \in \mathbb{N}}$ and $\{z_n \in \{0,1\}^{p(n)}\}_{n \in \mathbb{N}}$

$$\{(z_n, E_e(x_n))_{e \leftarrow G(1^n)_1}\}_{n \in \mathbb{N}} \approx_c \{(z_n, E_e(y_n))_{e \leftarrow G(1^n)_1}\}_{n \in \mathbb{N}}$$

- Non-uniform definition

Indistinguishablity of encryptions – private-key model

Definition 3 (Indistinguishablity of encryptions – private-key model)

An encryption scheme $(\mathsf{G},\mathsf{E},\mathsf{D})$ has indistinguishable encryptions in the private-key model, if for any $p,\ell \in \text{poly}$, $\{x_n, y_n \in \{0,1\}^{\ell(n)}\}_{n\in\mathbb{N}}$ and $\{z_n \in \{0,1\}^{p(n)}\}_{n\in\mathbb{N}}$

$$\{(z_n, E_e(x_n))_{e\leftarrow G(1^n)_1}\}_{n\in\mathbb{N}} \approx_c \{(z_n, E_e(y_n))_{e\leftarrow G(1^n)_1}\}_{n\in\mathbb{N}}$$

- Non-uniform definition

Definition 3 (Indistinguishablity of encryptions – private-key model)

An encryption scheme $(\mathsf{G}, \mathsf{E}, \mathsf{D})$ has indistinguishable encryptions in the private-key model, if for any $p, \ell \in \text{poly}$, $\{x_n, y_n \in \{0,1\}^{\ell(n)}\}_{n\in\mathbb{N}}$ and $\{z_n \in \{0,1\}^{p(n)}\}_{n\in\mathbb{N}}$

$$\{(z_n, E_e(x_n))_{e\leftarrow G(1^n)_1}\}_{n\in\mathbb{N}} \approx_c \{(z_n, E_e(y_n))_{e\leftarrow G(1^n)_1}\}_{n\in\mathbb{N}}$$

- Non-uniform definition
- Public-key variant — the ensemble contains e

Equivalence of definitions

Theorem 4

An encryption scheme (G, E, D) *is semantically secure iff is has indistinguishable encryptions.*

Equivalence of definitions

Theorem 4

An encryption scheme (G, E, D) is semantically secure iff is has indistinguishable encryptions.

We prove the private key case

Indistinguishability $\Longrightarrow$ Semantic Security

Indistinguishability $\Longrightarrow$ Semantic Security

Fix $\mathcal{M}$, A, f and h, as in Definition 2.

Indistinguishability $\Longrightarrow$ Semantic Security

Fix $\mathcal{M}$, A, f and h, as in Definition 2.
We construct A′ as

Algorithm 5 (A′)

Input: 1^n, $1^{|m|}$ and $h(m)$

1. $e \leftarrow G(1^n)_1$
2. $c = E_e(1^{|m|})$
3. Output $\mathsf{A}(1^n, 1^{|m|}, h(m), c)$

Indistinguishability $\implies$ Semantic Security

Fix $\mathcal{M}$, A, f and h, as in Definition 2.
We construct A′ as

Algorithm 5 (A′)

Input: 1^n, $1^{|m|}$ and $h(m)$

1. $e \leftarrow G(1^n)_1$
2. $c = E_e(1^{|m|})$
3. Output $A(1^n, 1^{|m|}, h(m), c)$

Claim 6

A′ is a good simulator for A (according to Definition 2)

Proving Claim 6

For $n \in \mathbb{N}$, let

$$\delta(n) := \Big| \Pr_{m \leftarrow \mathcal{M}_n, e \leftarrow G(1^n)_1}[\mathsf{A}(1^n, 1^{|m|}, h(1^n, m), E_e(m)) = f(1^n, m)] - \Pr_{m \leftarrow \mathcal{M}_n}[\mathsf{A}'(1^n, 1^{|m|}, h(1^n, m)) = f(1^n, m)] \Big|$$

Proving Claim 6

For $n \in \mathbb{N}$, let

$$\delta(n) := \left| \Pr_{m \leftarrow \mathcal{M}_n, e \leftarrow G(1^n)_1}[\mathsf{A}(1^n, 1^{|m|}, h(1^n, m), E_e(m)) = f(1^n, m)] - \Pr_{m \leftarrow \mathcal{M}_n}[\mathsf{A}'(1^n, 1^{|m|}, h(1^n, m)) = f(1^n, m)] \right|$$

Claim 7

For every $n \in \mathbb{N}$, exists $x_n \in \mathrm{Supp}(\mathcal{M}_n)$ with

$$\delta(n) \leq \left| \Pr_{e \leftarrow G(1^n)_1}[\mathsf{A}(1^n, 1^{|x_n|}, h(1^n, x_n), E_e(x_n)) = f(1^n, x_n)] - \Pr[\mathsf{A}'(1^n, 1^{|x_n|}, h(1^n, x_n)) = f(1^n, x_n)] \right|$$

Proving Claim 6

For $n \in \mathbb{N}$, let

$$\delta(n) := \Big| \Pr_{m \leftarrow \mathcal{M}_n, e \leftarrow G(1^n)_1}[\mathsf{A}(1^n, 1^{|m|}, h(1^n, m), E_e(m)) = f(1^n, m)] - \Pr_{m \leftarrow \mathcal{M}_n}[\mathsf{A}'(1^n, 1^{|m|}, h(1^n, m)) = f(1^n, m)] \Big|$$

Claim 7

For every $n \in \mathbb{N}$, exists $x_n \in \mathrm{Supp}(\mathcal{M}_n)$ with

$$\delta(n) \leq \Big| \Pr_{e \leftarrow G(1^n)_1}[\mathsf{A}(1^n, 1^{|x_n|}, h(1^n, x_n), E_e(x_n)) = f(1^n, x_n)] - \Pr[\mathsf{A}'(1^n, 1^{|x_n|}, h(1^n, x_n)) = f(1^n, x_n)] \Big|$$

Proof: ?

Assume $\exists$ an infinite $\mathcal{I} \subseteq \mathbb{N}$ and $p \in \text{poly}$ s.t. $\delta(n) > 1/p(n)$ for every $n \in \mathcal{I}$.

Assume $\exists$ an infinite $\mathcal{I} \subseteq \mathbb{N}$ and $p \in \text{poly}$ s.t. $\delta(n) > 1/p(n)$ for every $n \in \mathcal{I}$.

The following algorithm contradicts the indistinguishability of $(\mathsf{G}, \mathsf{E}, \mathsf{D})$ with respect to $\mathcal{M} = \{(x_n, y_n = 1^{|x_n|})\}_{n\in\mathbb{N}}$ and $\{z_n = (1^n, 1^{|x_n|}, h(1^n, x_n), f(1^n, x_n))\}_{n\in\mathbb{N}}$.

Algorithm 8 (B)

Input: $z_n = (1^n, 1^{|x_n|}, h(1^n, x_n), f(1^n, x_n))$, c

Output 1 iff $\mathsf{A}(1^n, 1^{|x_n|}, h(x_n), c) = f(1^n, x_n)$

Semantic Security $\Longrightarrow$ Indistinguishability

Assume $\exists$ PPT B, $\{x_n, y_n \in \{0,1\}^{\ell(n)}\}_{n\in\mathbb{N}}$ an $\{z_n\}_{n\in\mathbb{N}}$ and infinite $\mathcal{I} \subseteq \mathbb{N}$, such that

$$\Pr_{e\leftarrow G(1^n)_1}[\mathsf{B}(z_n, E_e(x_n)) = 1] - \Pr_{e\leftarrow G(1^n)_1}[\mathsf{B}(z_n, E_e(y_n)) = 1] \geq \frac{1}{p(n)} \quad (1)$$

$\forall n \in \mathcal{I}$.

Semantic Security $\implies$ Indistinguishability

Assume $\exists$ PPT B, $\{x_n, y_n \in \{0,1\}^{\ell(n)}\}_{n\in\mathbb{N}}$ an $\{z_n\}_{n\in\mathbb{N}}$ and infinite $\mathcal{I} \subseteq \mathbb{N}$, such that

$$\Pr_{e\leftarrow G(1^n)_1}[\mathsf{B}(z_n, E_e(x_n)) = 1] - \Pr_{e\leftarrow G(1^n)_1}[\mathsf{B}(z_n, E_e(y_n)) = 1] \geq \frac{1}{p(n)} \quad (1)$$

$\forall n \in \mathcal{I}$.

Let $f(1^n, x_n) = 1$ and $f(1^n, y_n) = 0$, and let $\mathsf{B}'(t)$ output 1 if $\mathsf{B}(t) = 1$, and a random coin otherwise.

Semantic Security $\Longrightarrow$ Indistinguishability

Assume $\exists$ PPT B, $\{x_n, y_n \in \{0,1\}^{\ell(n)}\}_{n\in\mathbb{N}}$ an $\{z_n\}_{n\in\mathbb{N}}$ and infinite $\mathcal{I} \subseteq \mathbb{N}$, such that

$$\Pr_{e\leftarrow G(1^n)_1}[\mathsf{B}(z_n, E_e(x_n)) = 1] - \Pr_{e\leftarrow G(1^n)_1}[\mathsf{B}(z_n, E_e(y_n)) = 1] \geq \frac{1}{p(n)} \quad (1)$$

$\forall n \in \mathcal{I}$.

Let $f(1^n, x_n) = 1$ and $f(1^n, y_n) = 0$, and let $\mathsf{B}'(t)$ output 1 if $\mathsf{B}(t) = 1$, and a random coin otherwise.

Claim 9

$\forall n \in \mathcal{I}$ and $t_n \in \{x_n, y_n\}$

$$\Pr_{e\leftarrow G(1^n)_1}\left[\mathsf{B}'(z_n, E_e(t_n)) = f(1^n, t_n)\right] \geq \frac{1}{2} + \frac{1}{p(n)}$$

Semantic Security $\implies$ Indistinguishability

Assume $\exists$ PPT B, $\{x_n, y_n \in \{0,1\}^{\ell(n)}\}_{n\in\mathbb{N}}$ an $\{z_n\}_{n\in\mathbb{N}}$ and infinite $\mathcal{I} \subseteq \mathbb{N}$, such that

$$\Pr_{e\leftarrow G(1^n)_1}[\mathrm{B}(z_n, E_e(x_n)) = 1] - \Pr_{e\leftarrow G(1^n)_1}[\mathrm{B}(z_n, E_e(y_n)) = 1] \geq \frac{1}{p(n)} \quad (1)$$

$\forall n \in \mathcal{I}$.

Let $f(1^n, x_n) = 1$ and $f(1^n, y_n) = 0$, and let $\mathrm{B}'(t)$ output 1 if $\mathrm{B}(t) = 1$, and a random coin otherwise.

Claim 9

$\forall n \in \mathcal{I}$ and $t_n \in \{x_n, y_n\}$

$$\Pr_{e\leftarrow G(1^n)_1}\left[\mathrm{B}'(z_n, E_e(t_n)) = f(1^n, t_n)\right] \geq \frac{1}{2} + \frac{1}{p(n)}$$

Proof?

- Let $\mathcal{M}_n$ be x_n wp $\frac{1}{2}$ and y_n otherwise.
- Let $f(1^n, x_n) = 1$, $f(1^n, y_n) = 0$ and $h(1^n, \cdot) = z_n$.
- Define $\mathsf{A}(1^n, 1^{\ell(n)}, z_n, c)$ to return $\mathsf{B}'(z_n, c)$.

- Let $\mathcal{M}_n$ be x_n wp $\frac{1}{2}$ and y_n otherwise.
- Let $f(1^n, x_n) = 1$, $f(1^n, y_n) = 0$ and $h(1^n, \cdot) = z_n$.
- Define $\mathsf{A}(1^n, 1^{\ell(n)}, z_n, c)$ to return $\mathsf{B}'(z_n, c)$.

By Claim 9

$$\Pr_{m \leftarrow \mathcal{M}_n, e \leftarrow G(1^n)_1}\left[\mathsf{A}(1^n, 1^{|m|}, h(1^n, m), E_e(m)) = f(1^n, m)\right] \geq \frac{1}{2} + \frac{1}{p(n)} \tag{2}$$

$\forall n \in \mathcal{I}$.

- Let $\mathcal{M}_n$ be x_n wp $\frac{1}{2}$ and y_n otherwise.
- Let $f(1^n, x_n) = 1$, $f(1^n, y_n) = 0$ and $h(1^n, \cdot) = z_n$.
- Define $\mathsf{A}(1^n, 1^{\ell(n)}, z_n, c)$ to return $\mathsf{B}'(z_n, c)$.

By Claim 9

$$\Pr_{m \leftarrow \mathcal{M}_n, e \leftarrow G(1^n)_1}\left[\mathsf{A}(1^n, 1^{|m|}, h(1^n, m), E_e(m)) = f(1^n, m)\right] \geq \frac{1}{2} + \frac{1}{p(n)} \tag{2}$$

$\forall n \in \mathcal{I}$.

But

$$\Pr_{m \leftarrow \mathcal{M}_n, e \leftarrow G(1^n)_1}\left[\mathsf{A}'(1^n, 1^{|m|}, h(1^n, m)) = f(1^n, m)\right] \leq \frac{1}{2} \tag{3}$$

for any A' and any $n \in \mathbb{N}$

Security Under Multiple Encryptions

Security Under Multiple Encryptions

Definition 10 (Indistinguishablity for multiple encryptions – private-key model)

An encryption scheme $(\mathsf{G}, \mathsf{E}, \mathsf{D})$ has indistinguishable encryptions for multiple messages in the private-key model, if for any $p, \ell, t \in \mathrm{poly}$, $\{x_{n,1}, \ldots x_{n,t(n)}, y_{n,1}, \ldots, y_{n,t(n)} \in \{0,1\}^{\ell(n)}\}_{n\in\mathbb{N}}$, $\{z_n \in \{0,1\}^{p(n)}\}_{n\in\mathbb{N}}$ and PPTM B,

$$\Big| \Pr_{e \leftarrow G(1^n)_1}[\mathsf{B}(z_n, E_e(x_{n,1}), \ldots E_e(x_{n,t(n)})) = 1] - \Pr_{e \leftarrow G(1^n)_1}[\mathsf{B}(z_n, E_e(y_{n,1}), \ldots E_e(y_{n,t(n)})) = 1 \Big| = \mathrm{neg}(n)$$

Security Under Multiple Encryptions

Definition 10 (Indistinguishablity for multiple encryptions – private-key model)

An encryption scheme $(\mathsf{G}, \mathsf{E}, \mathsf{D})$ has indistinguishable encryptions for multiple messages in the private-key model, if for any $p, \ell, t \in \mathrm{poly}$, $\{x_{n,1}, \ldots x_{n,t(n)}, y_{n,1}, \ldots, y_{n,t(n)} \in \{0,1\}^{\ell(n)}\}_{n \in \mathbb{N}}$, $\{z_n \in \{0,1\}^{p(n)}\}_{n \in \mathbb{N}}$ and PPTM B,

$$\left| \Pr_{e \leftarrow G(1^n)_1}[\mathsf{B}(z_n, E_e(x_{n,1}), \ldots E_e(x_{n,t(n)})) = 1] - \Pr_{e \leftarrow G(1^n)_1}[\mathsf{B}(z_n, E_e(y_{n,1}), \ldots E_e(y_{n,t(n)})) = 1 \right| = \mathrm{neg}(n)$$

Extensions:

- Different length messages

Definition 10 (Indistinguishablity for multiple encryptions – private-key model)

An encryption scheme (G, E, D) has indistinguishable encryptions for multiple messages in the private-key model, if for any $p, \ell, t \in$ poly, $\{x_{n,1}, \ldots x_{n,t(n)}, y_{n,1}, \ldots, y_{n,t(n)} \in \{0,1\}^{\ell(n)}\}_{n\in\mathbb{N}}$, $\{z_n \in \{0,1\}^{p(n)}\}_{n\in\mathbb{N}}$ and PPTM B,

$$\Big| \Pr_{e \leftarrow G(1^n)_1}[B(z_n, E_e(x_{n,1}), \ldots E_e(x_{n,t(n)})) = 1] - \Pr_{e \leftarrow G(1^n)_1}[B(z_n, E_e(y_{n,1}), \ldots E_e(y_{n,t(n)})) = 1 \Big| = \operatorname{neg}(n)$$

Extensions:

- Different length messages
- Semantic security version

Security Under Multiple Encryptions

Definition 10 (Indistinguishablity for multiple encryptions – private-key model)

An encryption scheme $(\mathsf{G}, \mathsf{E}, \mathsf{D})$ has indistinguishable encryptions for multiple messages in the private-key model, if for any $p, \ell, t \in \mathrm{poly}$, $\{x_{n,1}, \ldots x_{n,t(n)}, y_{n,1}, \ldots, y_{n,t(n)} \in \{0,1\}^{\ell(n)}\}_{n\in\mathbb{N}}$, $\{z_n \in \{0,1\}^{p(n)}\}_{n\in\mathbb{N}}$ and PPTM B,

$$\Big| \Pr_{e \leftarrow G(1^n)_1}[\mathsf{B}(z_n, E_e(x_{n,1}), \ldots E_e(x_{n,t(n)})) = 1] - \Pr_{e \leftarrow G(1^n)_1}[\mathsf{B}(z_n, E_e(y_{n,1}), \ldots E_e(y_{n,t(n)})) = 1 \Big| = \mathrm{neg}(n)$$

Extensions:

- Different length messages
- Semantic security version
- Public-key definition

Multiple Encryption in the Public-Key Model

Theorem 11

A public-key encryption scheme has indistinguishable encryptions for multiple messages, iff it has indistinguishable encryptions for a single message.

Multiple Encryption in the Public-Key Model

Theorem 11

A public-key encryption scheme has indistinguishable encryptions for multiple messages, iff it has indistinguishable encryptions for a single message.

Proof: Assume (G, E, D) is public-key secure for a single message and not for multiple messages with respect to B,
$\{x_{n,1}, \ldots x_{n,t(n)}, y_{n,1}, \ldots, y_{n,t(n)} \in \{0,1\}^{\ell(n)}\}_{n \in \mathbb{N}}$, $\{z_n \in \{0,1\}^{p(n)}\}_{n \in \mathbb{N}}$.

Multiple Encryption in the Public-Key Model

Theorem 11

A public-key encryption scheme has indistinguishable encryptions for multiple messages, iff it has indistinguishable encryptions for a single message.

Proof: Assume (G, E, D) is public-key secure for a single message and not for multiple messages with respect to B,
$\{x_{n,1}, \ldots x_{n,t(n)}, y_{n,1}, \ldots, y_{n,t(n)} \in \{0,1\}^{\ell(n)}\}_{n \in \mathbb{N}}$, $\{z_n \in \{0,1\}^{p(n)}\}_{n \in \mathbb{N}}$.
It follows that for some function $i(n) \in [t(n)]$

$$\begin{aligned} &\big|\Pr[B(1^n, e, E_e(x_{n,1}), \ldots, E_e(x_{n,i-1}), E_e(y_{n,i}) \ldots, E_e(y_{n,t(n)})) = 1] \\ &- \Pr[B(1^n, e, E_e(x_{n,1}), \ldots, E_e(x_{n,i}), E_e(y_{n,i+1}) \ldots, E_e(y_{n,t(n)})) = 1]\big| \\ &> \mathrm{neg}(n) \end{aligned}$$

where in both cases $e \leftarrow G(1^n)_1$

Algorithm 12 (B′)

Input: 1^n, $z_n = (i(n), x_{n,1}, \ldots x_{n,t(n)}, y_{n,1}, \ldots, y_{n,t(n)})$, e ,c
Return $\mathsf{B}(c, E_e(x_{n,1}), \ldots, E_e(x_{n,i-1}), c, E_e(y_{n,i+1}) \ldots, E_e(y_{n,t(n)}))$

Algorithm 12 (B')

Input: 1^n, $z_n = (i(n), x_{n,1}, \ldots x_{n,t(n)}, y_{n,1}, \ldots, y_{n,t(n)})$, e ,c
Return $\mathsf{B}(c, E_e(x_{n,1}), \ldots, E_e(x_{n,i-1}), c, E_e(y_{n,i+1}) \ldots, E_e(y_{n,t(n)}))$

B' is critically using the public key

Multiple Encryption in the Private-Key Model

Fact 13

Assuming (non uniform) OWFs exists, there exists an encryption scheme that has private-key indistinguishable encryptions for a single messages, but not for multiple messages

Multiple Encryption in the Private-Key Model

Fact 13

Assuming (non uniform) OWFs exists, there exists an encryption scheme that has private-key indistinguishable encryptions for a single messages, but not for multiple messages

Proof: Let $g\colon \{0,1\}^n \mapsto \{0,1\}^{n+1}$ be a (non-uniform) PRG, and for $i \in \mathbb{N}$ let g^i be its "iterated extension" to output of length $n + i$ (see Lecture 2, Construction 15).

Multiple Encryption in the Private-Key Model

Fact 13

Assuming (non uniform) OWFs exists, there exists an encryption scheme that has private-key indistinguishable encryptions for a single messages, but not for multiple messages

Proof: Let $g\colon \{0,1\}^n \mapsto \{0,1\}^{n+1}$ be a (non-uniform) PRG, and for $i \in \mathbb{N}$ let g^i be its "iterated extension" to output of length $n+i$ (see Lecture 2, Construction 15).

Construction 14

- $\mathsf{G}(1^n)$ outputs $e \leftarrow \{0,1\}^n$,
- $\mathsf{E}_e(m)$ outputs $g^{|m|}(e) \oplus m$
- $\mathsf{D}_e(c)$ outputs $g^{|c|}(e) \oplus c$

Claim 15

(G, E, D) has private-key indistinguishable encryptions for a single message

Proof:

Claim 15

$(\mathsf{G}, \mathsf{E}, \mathsf{D})$ has private-key indistinguishable encryptions for a single message

Proof: Assume not, and let B, $\{x_n, y_n \in \{0,1\}^{\ell(n)}\}_{n\in\mathbb{N}}$ and $\{z_n \in \{0,1\}^{p(n)}\}_{n\in\mathbb{N}}$ be the triplet that realizes it.

Claim 15

$(\mathsf{G}, \mathsf{E}, \mathsf{D})$ has private-key indistinguishable encryptions for a single message

Proof: Assume not, and let B, $\{x_n, y_n \in \{0,1\}^{\ell(n)}\}_{n\in\mathbb{N}}$ and $\{z_n \in \{0,1\}^{p(n)}\}_{n\in\mathbb{N}}$ be the triplet that realizes it. Namely,

$$\left|\Pr[\mathsf{B}(z_n, g^{\ell(n)}(U_n) \oplus x_n) = 1] - \Pr[\mathsf{B}(z_n, g^{\ell(n)}(U_n) \oplus y_n) = 1]\right| > \operatorname{neg}(n) \tag{4}$$

Claim 15

$(\mathsf{G}, \mathsf{E}, \mathsf{D})$ has private-key indistinguishable encryptions for a single message

Proof: Assume not, and let B, $\{x_n, y_n \in \{0,1\}^{\ell(n)}\}_{n\in\mathbb{N}}$ and $\{z_n \in \{0,1\}^{p(n)}\}_{n\in\mathbb{N}}$ be the triplet that realizes it. Namely,

$$\left|\Pr[\mathsf{B}(z_n, g^{\ell(n)}(U_n) \oplus x_n) = 1] - \Pr[\mathsf{B}(z_n, g^{\ell(n)}(U_n) \oplus y_n) = 1]\right| > \mathrm{neg}(n) \tag{4}$$

Hence, B yields a (non-uniform) distinguisher for g

Claim 15

(G, E, D) has private-key indistinguishable encryptions for a single message

Proof: Assume not, and let B, $\{x_n, y_n \in \{0,1\}^{\ell(n)}\}_{n\in\mathbb{N}}$ and $\{z_n \in \{0,1\}^{p(n)}\}_{n\in\mathbb{N}}$ be the triplet that realizes it. Namely,

$$\left|\Pr[\mathsf{B}(z_n, g^{\ell(n)}(U_n) \oplus x_n) = 1] - \Pr[\mathsf{B}(z_n, g^{\ell(n)}(U_n) \oplus y_n) = 1]\right| > \mathrm{neg}(n) \tag{4}$$

Hence, B yields a (non-uniform) distinguisher for g

Claim 16

(G, E, D) does not have a private-key indistinguishable encryptions for multiple messages

Claim 15

$(\mathsf{G}, \mathsf{E}, \mathsf{D})$ has private-key indistinguishable encryptions for a single message

Proof: Assume not, and let B, $\{x_n, y_n \in \{0,1\}^{\ell(n)}\}_{n\in\mathbb{N}}$ and $\{z_n \in \{0,1\}^{p(n)}\}_{n\in\mathbb{N}}$ be the triplet that realizes it. Namely,

$$\left|\Pr[\mathsf{B}(z_n, g^{\ell(n)}(U_n) \oplus x_n) = 1] - \Pr[\mathsf{B}(z_n, g^{\ell(n)}(U_n) \oplus y_n) = 1]\right| > \operatorname{neg}(n) \tag{4}$$

Hence, B yields a (non-uniform) distinguisher for g

Claim 16

$(\mathsf{G}, \mathsf{E}, \mathsf{D})$ does not have a private-key indistinguishable encryptions for multiple messages

Proof:

Claim 15

$(\mathsf{G}, \mathsf{E}, \mathsf{D})$ has private-key indistinguishable encryptions for a single message

Proof: Assume not, and let B, $\{x_n, y_n \in \{0,1\}^{\ell(n)}\}_{n\in\mathbb{N}}$ and $\{z_n \in \{0,1\}^{p(n)}\}_{n\in\mathbb{N}}$ be the triplet that realizes it. Namely,

$$\left|\Pr[\mathsf{B}(z_n, g^{\ell(n)}(U_n) \oplus x_n) = 1] - \Pr[\mathsf{B}(z_n, g^{\ell(n)}(U_n) \oplus y_n) = 1]\right| > \operatorname{neg}(n) \tag{4}$$

Hence, B yields a (non-uniform) distinguisher for g

Claim 16

$(\mathsf{G}, \mathsf{E}, \mathsf{D})$ does not have a private-key indistinguishable encryptions for multiple messages

Proof: Take $x_{n,1} = x_{n,2}$, $y_{n,1} \neq y_{n,2}$ and let B be the algorithm that on input (c_1, c_2), outputs 1 iff $c_1 = c_2$.

Section 2

Constructions

Private key indistinguishable encryptions for multiple messages

Suffice to encrypt messages of some fixed length (here the length is n).

Private key indistinguishable encryptions for multiple messages

Suffice to encrypt messages of some fixed length (here the length is n).

Let $\mathcal{F}$ be a (non-uniform) length preserving PRF

Private key indistinguishable encryptions for multiple messages

Suffice to encrypt messages of some fixed length (here the length is n).
Let $\mathcal{F}$ be a (non-uniform) length preserving PRF

Construction 17

- $\mathsf{G}(1^n)$: output $e \leftarrow \mathcal{F}_n$,
- $\mathsf{E}_e(m)$: choose $r \leftarrow \{0,1\}^n$ and output $(r, e(r) \oplus m)$
- $\mathsf{D}_e(r,c)$: output $e(r) \oplus c$

Private key indistinguishable encryptions for multiple messages

Suffice to encrypt messages of some fixed length (here the length is n).
Let $\mathcal{F}$ be a (non-uniform) length preserving PRF

Construction 17

- $\mathsf{G}(1^n)$: output $e \leftarrow \mathcal{F}_n$,
- $\mathsf{E}_e(m)$: choose $r \leftarrow \{0,1\}^n$ and output $(r, e(r) \oplus m)$
- $\mathsf{D}_e(r,c)$: output $e(r) \oplus c$

Claim 18

$(\mathsf{G}, \mathsf{E}, \mathsf{D})$ has private-key indistinguishable encryptions for a multiple messages

Private key indistinguishable encryptions for multiple messages

Suffice to encrypt messages of some fixed length (here the length is n).
Let $\mathcal{F}$ be a (non-uniform) length preserving PRF

Construction 17

- $\mathsf{G}(1^n)$: output $e \leftarrow \mathcal{F}_n$,
- $\mathsf{E}_e(m)$: choose $r \leftarrow \{0,1\}^n$ and output $(r, e(r) \oplus m)$
- $\mathsf{D}_e(r,c)$: output $e(r) \oplus c$

Claim 18

$(\mathsf{G}, \mathsf{E}, \mathsf{D})$ has private-key indistinguishable encryptions for a multiple messages

Proof:

Public-key indistinguishable encryptions for multiple messages

Let (G, f, Inv) be a (non-uniform) TDP, and let b be an hardcore predicate for it.

Public-key indistinguishable encryptions for multiple messages

Let (G, f, Inv) be a (non-uniform) TDP, and let b be an hardcore predicate for it.

Construction 19 (bit encryption)

- $\mathsf{G}(1^n)$: output $(e, d) \leftarrow \mathsf{G}(1^n)$
- $\mathsf{E}_e(m)$: choose $r \leftarrow \{0,1\}^n$ and output $(y = f_e(r), c = b(r) \oplus m)$
- $\mathsf{D}_d(y, c)$: output $b(\text{Inv}_d(y)) \oplus c$

Public-key indistinguishable encryptions for multiple messages

Let (G, f, Inv) be a (non-uniform) TDP, and let b be an hardcore predicate for it.

Construction 19 (bit encryption)

- $\mathrm{G}(1^n)$: output $(e, d) \leftarrow \mathrm{G}(1^n)$
- $\mathrm{E}_e(m)$: choose $r \leftarrow \{0,1\}^n$ and output $(y = f_e(r), c = b(r) \oplus m)$
- $\mathrm{D}_d(y, c)$: output $b(\mathrm{Inv}_d(y)) \oplus c$

Claim 20

$(\mathrm{G}, \mathrm{E}, \mathrm{D})$ has public-key indistinguishable encryptions for a multiple messages

Public-key indistinguishable encryptions for multiple messages

Let (G, f, Inv) be a (non-uniform) TDP, and let b be an hardcore predicate for it.

Construction 19 (bit encryption)

- $\mathrm{G}(1^n)$: output $(e, d) \leftarrow \mathrm{G}(1^n)$
- $\mathrm{E}_e(m)$: choose $r \leftarrow \{0,1\}^n$ and output $(y = f_e(r), c = b(r) \oplus m)$
- $\mathrm{D}_d(y, c)$: output $b(\mathrm{Inv}_d(y)) \oplus c$

Claim 20

$(\mathrm{G}, \mathrm{E}, \mathrm{D})$ has public-key indistinguishable encryptions for a multiple messages

- We believe that public-key encryptions schemes are “more complex" than private-key ones

Section 3

Active Adversaries

Active Adversaries

- Chosen plaintext attack (CPA):
  The adversary can ask for encryption and choose the messages to distinguish accordingly

Active Adversaries

- Chosen plaintext attack (CPA):
  The adversary can ask for encryption and choose the messages to distinguish accordingly
- Chosen ciphertext attack (CCA):
  The adversary can also ask for decryptions of certain messages

Active Adversaries

- Chosen plaintext attack (CPA):
  The adversary can ask for encryption and choose the messages to distinguish accordingly
- Chosen ciphertext attack (CCA):
  The adversary can also ask for decryptions of certain messages

Active Adversaries

- Chosen plaintext attack (CPA):
  The adversary can ask for encryption and choose the messages to distinguish accordingly
- Chosen ciphertext attack (CCA):
  The adversary can also ask for decryptions of certain messages
- In the public-key settings, the adversary is also given the public key

Active Adversaries

- Chosen plaintext attack (CPA):
  The adversary can ask for encryption and choose the messages to distinguish accordingly
- Chosen ciphertext attack (CCA):
  The adversary can also ask for decryptions of certain messages
- In the public-key settings, the adversary is also given the public key

Active Adversaries

- Chosen plaintext attack (CPA):
  The adversary can ask for encryption and choose the messages to distinguish accordingly
- Chosen ciphertext attack (CCA):
  The adversary can also ask for decryptions of certain messages

- In the public-key settings, the adversary is also given the public key
- We focus on indistinguishability, but each of the above definitions has an equivalent semantic security variant.

CPA Security

Let $(\mathsf{G}, \mathsf{E}, \mathsf{D})$ be an encryption scheme. For a pair of algorithms $\mathsf{A} = (\mathsf{A}_1, \mathsf{A}_2)$, $n \in \mathbb{N}$, $z \in \{0,1\}^*$ and $b \in \{0,1\}$, let:

Experiment 21 ($\mathsf{Exp}^{\mathsf{CPA}}_{\mathsf{A},n,z}(b)$)

1. $(e, d) \leftarrow G(1^n)$
2. $(m_0, m_1, s) \leftarrow \mathsf{A}_1^{E_e(\cdot)}(1^n, z)$
3. $c \leftarrow \mathsf{E}_e(m_b)$
4. Output $\mathsf{A}_2^{E_e(\cdot)}(1^n, s, c)$

CPA Security

Let $(\mathsf{G}, \mathsf{E}, \mathsf{D})$ be an encryption scheme. For a pair of algorithms $\mathsf{A} = (\mathsf{A}_1, \mathsf{A}_2)$, $n \in \mathbb{N}$, $z \in \{0,1\}^*$ and $b \in \{0,1\}$, let:

Experiment 21 ($\mathsf{Exp}^{\mathsf{CPA}}_{\mathsf{A},n,z}(b)$)

1. $(e, d) \leftarrow G(1^n)$
2. $(m_0, m_1, s) \leftarrow \mathsf{A}_1^{E_e(\cdot)}(1^n, z)$
3. $c \leftarrow \mathsf{E}_e(m_b)$
4. Output $\mathsf{A}_2^{E_e(\cdot)}(1^n, s, c)$

Definition 22 (private key CPA)

$(\mathsf{G}, \mathsf{E}, \mathsf{D})$ has indistinguishable encryptions in the private-key model under CPA attack, if $\forall$ PPT $\mathsf{A}_1, \mathsf{A}_2$, and poly-bounded $\{z_n\}_{n \in \mathbb{N}}$:

$$|\Pr[\mathsf{Exp}^{\mathsf{CPA}}_{\mathsf{A},n,z_n}(0) = 1] - \Pr[\mathsf{Exp}^{\mathsf{CPA}}_{\mathsf{A},n,z_n}(1) = 1]| = \mathsf{neg}(n)$$

- public-key variant...

- public-key variant...
- The scheme from Construction 17 has indistinguishable encryptions in the private-key model under CPA attack (for short, private-key CPA secure)

- public-key variant...
- The scheme from Construction 17 has indistinguishable encryptions in the private-key model under CPA attack (for short, private-key CPA secure)
- The scheme from Construction 19 has indistinguishable encryptions in the public-key model under CPA attack (for short, public-key CPA secure)

- public-key variant...
- The scheme from Construction 17 has indistinguishable encryptions in the private-key model under CPA attack (for short, private-key CPA secure)
- The scheme from Construction 19 has indistinguishable encryptions in the public-key model under CPA attack (for short, public-key CPA secure)
- In both cases, definitions are not equivalent

CCA Security

Experiment 23 ($\mathrm{Exp}^{\mathrm{CCA1}}_{\mathsf{A},n,z}(b)$)

1. $(e, d) \leftarrow G(1^n)$
2. $(m_0, m_1, s) \leftarrow \mathsf{A}_1^{E_e(\cdot), D_d(\cdot)}(1^n, z)$
3. $c \leftarrow \mathsf{E}_e(m_b)$
4. Output $\mathsf{A}_2^{E_e(\cdot)}(1^n, s, c)$

CCA Security

Experiment 23 ($\mathrm{Exp}^{\mathrm{CCA1}}_{\mathsf{A},n,z}(b)$)

1. $(e, d) \leftarrow G(1^n)$
2. $(m_0, m_1, s) \leftarrow \mathsf{A}_1^{E_e(\cdot), D_d(\cdot)}(1^n, z)$
3. $c \leftarrow \mathsf{E}_e(m_b)$
4. Output $\mathsf{A}_2^{E_e(\cdot)}(1^n, s, c)$

Experiment 24 ($\mathrm{Exp}^{\mathrm{CCA2}}_{\mathsf{A},n,z_n}(b)$)

1. $(e, d) \leftarrow G(1^n)$
2. $(x_0, x_1, s) \leftarrow \mathsf{A}_1^{E_e(\cdot), D_d(\cdot)}(1^n, z)$
3. $c \leftarrow \mathsf{E}_e(x_b)$
4. Output $\mathsf{A}_2^{E_e(\cdot), D_d^{\neg c}(\cdot)}(1^n, s, c)$

Definition 25 (private key CCA1/CCA2)

$(\mathsf{G}, \mathsf{E}, \mathsf{D})$ has indistinguishable encryptions in the private-key model under $x \in \{\mathsf{CCA1}, \mathsf{CCA2}\}$ attack, if $\forall$ PPT $\mathsf{A}_1, \mathsf{A}_2$, and poly-bounded $\{z_n\}_{n \in \mathbb{N}}$:

$$|\Pr[\mathsf{Exp}^x_{\mathsf{A},n,z_n}(0) = 1] - \Pr[\mathsf{Exp}^x_{\mathsf{A},n,z_n}(1) = 1]| = \mathsf{neg}(n)$$

Definition 25 (private key CCA1/CCA2)

(G, E, D) has indistinguishable encryptions in the private-key model under $x \in \{\mathrm{CCA1}, \mathrm{CCA2}\}$ attack, if $\forall$ PPT A_1, A_2, and poly-bounded $\{z_n\}_{n\in\mathbb{N}}$:

$$|\Pr[\mathrm{Exp}^{x}_{A,n,z_n}(0) = 1] - \Pr[\mathrm{Exp}^{x}_{A,n,z_n}(1) = 1]| = \mathrm{neg}(n)$$

- The public key definition is analogous

Private-key CCA2

- Is the scheme from Construction 17 private-key CCA1 secure?

Private-key CCA2

- Is the scheme from Construction 17 private-key CCA1 secure?
- CCA2 secure?

Private-key CCA2

- Is the scheme from Construction 17 private-key CCA1 secure?
- CCA2 secure?

Private-key CCA2

- Is the scheme from Construction 17 private-key CCA1 secure?
- CCA2 secure?

Let $(\mathsf{G}, \mathsf{E}, \mathsf{D})$ be a private key CPA scheme, and let $(\mathsf{Gen}_M, \mathsf{Mac}, \mathsf{Vrfy})$ be an existential unforgeable strong MAC.

Construction 26

- $\mathsf{G}'(1^n)$: Output $(e \leftarrow \mathsf{G}_E(1^n), k \leftarrow \mathsf{Gen}_M(1^n))$.[a]
- $\mathsf{E}'_{e,k}(m)$: let $c = \mathsf{E}_e(m)$ and output $(c, t = \mathsf{Mac}_k(c))$
- $\mathsf{D}_{e,k}(c, t)$: if $\mathsf{Vrfy}_k(c, t) = 1$, output $\mathsf{D}_e(c)$. Otherwise, output $\perp$

[a] We assume for simplicity that the encryption and decryption keys are the same.

Private-key CCA2

- Is the scheme from Construction 17 private-key CCA1 secure?
- CCA2 secure?

Let (G, E, D) be a private key CPA scheme, and let $(\mathrm{Gen}_M, \mathrm{Mac}, \mathrm{Vrfy})$ be an existential unforgeable strong MAC.

Construction 26

- $G'(1^n)$: Output $(e \leftarrow G_E(1^n), k \leftarrow \mathrm{Gen}_M(1^n))$.[a]
- $E'_{e,k}(m)$: let $c = E_e(m)$ and output $(c, t = \mathrm{Mac}_k(c))$
- $D_{e,k}(c,t)$: if $\mathrm{Vrfy}_k(c,t) = 1$, output $D_e(c)$. Otherwise, output $\perp$

[a] We assume for simplicity that the encryption and decryption keys are the same.

Theorem 27

Construction 26 is a private-key CCA2-secure encryption scheme.

Theorem 27

Construction 26 is a private-key CCA2-secure encryption scheme.

Proof: ?

Public-key CCA1

Public-key CCA1

Let $(\mathsf{G}, \mathsf{E}, \mathsf{D})$ be a public-key CPA scheme and let (P, V) be a $\mathcal{NIZK}$ for $\mathcal{L} = \{(c_0, c_1, pk_0, pk_1) \colon \exists (m, z_0, z_1) \quad \text{s.t.} \quad c_0 = \mathsf{E}_{pk_0}(m, z_0) \wedge c_1 = \mathsf{E}_{pk_1}(m, z_1)\}$

Public-key CCA1

Let $(\mathsf{G}, \mathsf{E}, \mathsf{D})$ be a public-key CPA scheme and let (P, V) be a $\mathcal{NIZK}$ for $\mathcal{L} = \{(c_0, c_1, pk_0, pk_1) \colon \exists (m, z_0, z_1) \text{ s.t. } c_0 = \mathsf{E}_{pk_0}(m, z_0) \wedge c_1 = \mathsf{E}_{pk_1}(m, z_1)\}$

Construction 28 (The Naor-Yung Paradigm)

- $\mathsf{G}'(1^n)$:
  1. For $i \in \{0, 1\}$: set $(sk_i, pk_i) \leftarrow \mathsf{G}(1^n)$.
  2. Let $r \leftarrow \{0, 1\}^{\ell(n)}$, and output $pk' = (pk_0, pk_1, r)$ and $sk' = (pk', sk_0, sk_1)$
- $\mathsf{E}'_{pk'}(m)$:
  1. For $i \in \{0, 1\}$: $c_i = \mathsf{E}_{pk_i}(m, z_i)$, where z_i is a uniformly chosen string of the right length
  2. $\pi \leftarrow \mathsf{P}((c_0, c_1, pk_0, pk_1), (m, z_0, z_1), r)$
  3. Output (c_0, c_1, π).
- $\mathsf{D}'_{sk'}(c_0, c_1, \pi)$: If $\mathsf{V}((c_0, c_1, pk_0, pk_1), \pi, r) = 1$, return $\mathsf{D}_{sk_0}(c_0)$. Otherwise, return $\perp$

Omitted details:

- We assume for simplicity that the encryption key output by $\mathsf{G}(1^n)$ is of length at least n.
- ℓ is an arbitrary polynomial, and determines the maximum message length to encrypt using ”security parameter" n.

Omitted details:

- We assume for simplicity that the encryption key output by $G(1^n)$ is of length at least n.
- ℓ is an arbitrary polynomial, and determines the maximum message length to encrypt using ”security parameter" n.

Is the scheme CCA1 secure?

Omitted details:

- We assume for simplicity that the encryption key output by $\mathsf{G}(1^n)$ is of length at least n.
- ℓ is an arbitrary polynomial, and determines the maximum message length to encrypt using ”security parameter" n.

Is the scheme CCA1 secure? We need the $\mathcal{NIZK}$ to be “adaptive secure".

Theorem 29

Assuming that (P, V) is adaptive secure, then Construction 28 is a public-key CCA1 secure encryption scheme.

Omitted details:

- We assume for simplicity that the encryption key output by $\mathsf{G}(1^n)$ is of length at least n.
- ℓ is an arbitrary polynomial, and determines the maximum message length to encrypt using "security parameter" n.

Is the scheme CCA1 secure? We need the $\mathcal{NIZK}$ to be "adaptive secure".

Theorem 29

Assuming that (P, V) is adaptive secure, then Construction 28 is a public-key CCA1 secure encryption scheme.

Proof: Given an attacker A' for the CCA1 security of $(\mathsf{G}', \mathsf{E}', \mathsf{D}')$, we use it to construct an attacker A on the CPA security of $(\mathsf{G}, \mathsf{E}, \mathsf{D})$.

Let $\mathsf{S} = (\mathsf{S}_1, \mathsf{S}_2)$ be the (adaptive) simulator for $(\mathsf{P}, \mathsf{V}, \mathcal{L})$

Let $\mathsf{S} = (\mathsf{S}_1, \mathsf{S}_2)$ be the (adaptive) simulator for $(\mathsf{P}, \mathsf{V}, \mathcal{L})$

Algorithm 30 (A)

Input: $(1^n, pk)$

1. let $j \leftarrow \{0,1\}$, $pk_{1-j} = pk$, $(pk_j, sk_j) \leftarrow \mathsf{G}(1^n)$ and $(r, s) \leftarrow \mathsf{S}_1(1^n)$
2. Emulate $\mathsf{A}'(1^n, pk' = (pk_0, pk_1, r))$ as follows:
3. On query (c_0, c_1, π) of A' to D':
   If $\mathsf{V}((c_0, c_1, pk_0, pk_1), \pi, r) = 1$, answer $\mathsf{D}_{sk_j}(c_j)$.
   Otherwise, answer $\perp$.
4. Output the same pair (m_0, m_1) as A' does
5. On challenge c ($= \mathsf{E}_{pk}(m_b)$):
   - Set $c_{1-j} = c$, $a \leftarrow \{0,1\}$, $c_j = \mathsf{E}_{pk_j}(m_a)$, and $\pi \leftarrow \mathsf{S}_2((c_0, c_1, pk_0, pk_1), r, s)$
   - Send $c' = (c_0, c_1, \pi)$ to A'
6. Output the same value that A' does

Claim 31

Assume that A' breaks the CCA1 security of (G', E', D') with probability $\delta(n)$, then A breaks the CPA security of (G, E, D) with probability $(\delta(n) - \mathrm{neg}(n))/2$.

Claim 31

Assume that A' breaks the CCA1 security of $(\mathsf{G}', \mathsf{E}', \mathsf{D}')$ with probability $\delta(n)$, then A breaks the CPA security of $(\mathsf{G}, \mathsf{E}, \mathsf{D})$ with probability $(\delta(n) - \mathrm{neg}(n))/2$.

The adaptive soundness and adaptive zero-knowledge of (P, V), yields that

$$\Pr[\mathsf{A}' \text{ “makes" } \mathsf{A}(1^n) \text{ decrypt an invalid cipher}] = \mathrm{neg}(n) \tag{5}$$

Claim 31

Assume that A' breaks the CCA1 security of (G', E', D') with probability $\delta(n)$, then A breaks the CPA security of (G, E, D) with probability $(\delta(n) - \mathrm{neg}(n))/2$.

The adaptive soundness and adaptive zero-knowledge of (P, V), yields that

$$\Pr[A' \text{ “makes" } A(1^n) \text{ decrypt an invalid cipher}] = \mathrm{neg}(n) \tag{5}$$

In the following we assume for simplicity that the above prob is 0.

Claim 31

Assume that A' breaks the CCA1 security of $(\mathsf{G}', \mathsf{E}', \mathsf{D}')$ with probability $\delta(n)$, then A breaks the CPA security of $(\mathsf{G}, \mathsf{E}, \mathsf{D})$ with probability $(\delta(n) - \operatorname{neg}(n))/2$.

The adaptive soundness and adaptive zero-knowledge of (P, V), yields that

$$\Pr[\mathsf{A}' \text{ “makes" } \mathsf{A}(1^n) \text{ decrypt an invalid cipher}] = \operatorname{neg}(n) \tag{5}$$

In the following we assume for simplicity that the above prob is 0.
Hence, no information about j has leaked to A through the first stage.

Claim 31

Assume that A' breaks the CCA1 security of $(\mathsf{G}', \mathsf{E}', \mathsf{D}')$ with probability $\delta(n)$, then A breaks the CPA security of $(\mathsf{G}, \mathsf{E}, \mathsf{D})$ with probability $(\delta(n) - \mathsf{neg}(n))/2$.

The adaptive soundness and adaptive zero-knowledge of (P, V), yields that

$$\Pr[\mathsf{A}' \text{ “makes" } \mathsf{A}(1^n) \text{ decrypt an invalid cipher}] = \mathsf{neg}(n) \qquad (5)$$

In the following we assume for simplicity that the above prob is 0. Hence, no information about j has leaked to A through the first stage.

Let $\mathsf{A}'(1^n, a^*, b^*)$ be the output of $\mathsf{A}'(1^n)$ in the emulation induced by A, where $a = a^*$ and $b = b^*$.

Claim 31

Assume that A' breaks the CCA1 security of $(\mathsf{G}', \mathsf{E}', \mathsf{D}')$ with probability $\delta(n)$, then A breaks the CPA security of $(\mathsf{G}, \mathsf{E}, \mathsf{D})$ with probability $(\delta(n) - \mathrm{neg}(n))/2$.

The adaptive soundness and adaptive zero-knowledge of (P, V), yields that

$$\Pr[\mathsf{A}' \text{ ``makes" } \mathsf{A}(1^n) \text{ decrypt an invalid cipher}] = \mathrm{neg}(n) \tag{5}$$

In the following we assume for simplicity that the above prob is 0. Hence, no information about j has leaked to A through the first stage.

Let $\mathsf{A}'(1^n, a^*, b^*)$ be the output of $\mathsf{A}'(1^n)$ in the emulation induced by A, where $a = a^*$ and $b = b^*$. It holds that

1. $\mathsf{A}'(1^n, 0, 1) \equiv \mathsf{A}'(1^n, 1, 0)$

Claim 31

Assume that A' breaks the CCA1 security of $(\mathsf{G}', \mathsf{E}', \mathsf{D}')$ with probability $\delta(n)$, then A breaks the CPA security of $(\mathsf{G}, \mathsf{E}, \mathsf{D})$ with probability $(\delta(n) - \operatorname{neg}(n))/2$.

The adaptive soundness and adaptive zero-knowledge of (P, V), yields that

$$\Pr[\mathsf{A}' \text{ “makes" } \mathsf{A}(1^n) \text{ decrypt an invalid cipher}] = \operatorname{neg}(n) \tag{5}$$

In the following we assume for simplicity that the above prob is 0. Hence, no information about j has leaked to A through the first stage.

Let $\mathsf{A}'(1^n, a^*, b^*)$ be the output of $\mathsf{A}'(1^n)$ in the emulation induced by A, where $a = a^*$ and $b = b^*$. It holds that

1. $\mathsf{A}'(1^n, 0, 1) \equiv \mathsf{A}'(1^n, 1, 0)$
2. The adaptive zero-knowledge of (P, V) yields that $|\Pr[\mathsf{A}'(1^n, 1, 1) = 1] - \Pr[\mathsf{A}'(1^n, 0, 0) = 1]| \geq \delta(n) - \operatorname{neg}(n)$

Let $\mathsf{A}(b)$ be the outputs of A when the challenge is b.

Let $\mathsf{A}(b)$ be the outputs of A when the challenge is b.

$$\begin{aligned}
&|\Pr[\mathsf{A}(1) = 1] - \Pr[\mathsf{A}(0) = 1]| \\
&\quad = |\frac{1}{2}(\Pr[\mathsf{A}'(0,1) = 1] + \Pr[\mathsf{A}'(1,1) = 1]) \\
&\qquad -\frac{1}{2}(\Pr[\mathsf{A}'(0,0) = 1] + \Pr[\mathsf{A}'(1,0) = 1])\Big|
\end{aligned}$$

Let $A(b)$ be the outputs of A when the challenge is b.

$$\begin{aligned}
&|\Pr[A(1) = 1] - \Pr[A(0) = 1]| \\
&\quad = |\frac{1}{2}(\Pr[A'(0,1) = 1] + \Pr[A'(1,1) = 1]) \\
&\qquad - \frac{1}{2}(\Pr[A'(0,0) = 1] + \Pr[A'(1,0) = 1])| \\
&\quad \geq \frac{1}{2}|\Pr[A'(1,1) = 1] - \Pr[A'(0,0) = 1]| \\
&\qquad - \frac{1}{2}|\Pr[A'(1,0) = 1] - \Pr[A'(0,1) = 1]|
\end{aligned}$$

Let $A(b)$ be the outputs of A when the challenge is b.

$$\begin{aligned}
&|\Pr[A(1) = 1] - \Pr[A(0) = 1]| \\
&\quad = |\frac{1}{2}(\Pr[A'(0,1) = 1] + \Pr[A'(1,1) = 1]) \\
&\qquad -\frac{1}{2}(\Pr[A'(0,0) = 1] + \Pr[A'(1,0) = 1])| \\
&\quad \geq \frac{1}{2}|\Pr[A'(1,1) = 1] - \Pr[A'(0,0) = 1]| \\
&\qquad -\frac{1}{2}|\Pr[A'(1,0) = 1] - \Pr[A'(0,1) = 1]| \\
&\quad \geq (\delta(n) - \mathrm{neg}(n))/2
\end{aligned}$$

Public-key CCA2

- Is Construction 28 CCA2 secure?

Public-key CCA2

- Is Construction 28 CCA2 secure?
- **Problem:** Soundness might not hold with respect to the simulated CRS, after seeing a proof for an invalid statement

Public-key CCA2

- Is Construction 28 CCA2 secure?
- **Problem:** Soundness might not hold with respect to the simulated CRS, after seeing a proof for an invalid statement
- **Solution:** use simulation sound $\mathcal{NIZK}$